Magistrate Judge David W. Christel

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. BHAVESH PATEL, Defendant.	CASE NO. MJ18-5116 COMPLAINT for VIOLATION Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i)(I), (II), (IV) and (VI) and (ii)

BEFORE, the Honorable David W. Christel, United States Magistrate Judge, U.S. Courthouse, Tacoma, Washington.

The undersigned complainant being duly sworn states:

COUNT 1

(Intentional Damage to a Protected Computer)

I. Introduction

At all times material to this Complaint:

1. The victim in this case was a Washington non-profit health-services company that operated hospitals and medical centers in the South Puget Sound area of Washington State (hereinafter, "Victim Hospital");

2. Victim Hospital operated a computer network with medical-service providers' workstations located in Pierce County, Washington;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

3. Defendant BHAVESH PATEL was an individual employed as a contractor for Victim Hospital as a lead database engineer and administrator responsible for implementing an electronic medical records system known as EPIC;

4. Defendant's project assignment at Victim Hospital was terminated on or about July 18, 2013, after which time he was not authorized to access Victim Hospital's computer systems.

II. The Offense

A. Patel's Unauthorized Access to Victim Hospital's Computers

5. On or about July 17, 2013, PATEL modified the user account of a former employee by changing the password;

6. On or about August 16, 2013, PATEL logged into a virtual private network (VPN) for Victim Hospital using an account in his name that established a connection between a computer at his home in South Dakota and Victim Hospital's network;

7. Upon logging into the VPN, PATEL then logged into Victim Hospital's system using the former employee's user account that he had reset on July 17, 2013;

8. While logged into Victim Hospital's system as the former employee, PATEL modified the system alert file that is used for the delivery of alert notifications to system administrators regarding problems with Victim Hospital's servers; PATEL changed the e-mail address to which alert messages are sent to a non-existent e-mail address. This action prevented system administrators from being able to receive alerts when subsequent system errors occurred;

9. PATEL then changed the "environment copy" script that was scheduled to run every night at 2:00 AM. By changing the script, PATEL caused the system to copy files including patient medical records and other data that belongs to Victim Hospital from support to production instead of from production to support. After PATEL modified the "environment copy" script, the script was configured to copy older copies of critical data files from the previous day's backup, overwriting the most current data files and losing any new or changed patient data from the preceding 24 hours;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

10. PATEL then changed the script schedule such that the modified "environment copy" script ran immediately rather than waiting until 2:00 AM the next day. When the modified script was executed, the system rejected the copy operation that the script attempted to perform. This in turn caused the system to enter an error state that made the system unavailable to the entire Victim Hospital system. System administrators were not alerted to the error condition by the system alert mechanism because PATEL had altered the alert configuration earlier;

11. After changing the environment copy script, PATEL used the set command to change the last modified date and time for the environment copy script and the log files that record when the environment copy script operated;

12. As a result of PATEL's changes to the environment copy script, the entire medical record system at four of the Victim Hospital's facilities in the Puget Sound region crashed for approximately 30 minutes preventing hospital personnel from accessing patient medical records, properly admitting new patients, or registering patient medications in the Victim Hospital's records system.

B. Execution of The Offense

On or about August 16, 2013, in Pierce County, within the Western District of Washington and elsewhere, the defendant, BHAVESH PATEL, knowingly caused the transmission of a program, information, code, and command, and, as a result of that conduct, intentionally caused, and attempted to cause, damage, without authorization, to a protected computer, to wit, by logging into Victim Hospital's computer system, changing the alert e-mail address, altering the environment copy script, changing the script schedule, and changing the last modified date and time for the script and log files, PATEL intentionally caused damage resulting in loss to one or more persons during a one-year period aggregating at least $5,000 in value; the modification and impairment, and potential modification and impairment, of the medical examination, diagnosis, treatment, and care of 1 or more individuals; a threat to public health and safety, and; damage affecting 10 or more protected computers during a one-year period.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i)(I), (II), (IV) and (VI) and (ii).

And the complainant states that this Complaint is based on the following information:

I, Michael D. Brown, being first duly sworn on oath, depose and say:

BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed for approximately ten and a half years. I am currently assigned to the Seattle Division's Tacoma Resident Agency. While employed by the FBI, I have investigated a variety of federal criminal violations, including mail and wire fraud, money laundering, public corruption, violent crime, and securities fraud. I have participated in the drafting and execution of numerous complaints and search warrants during my career. In addition to my experience, I have received specialized training from the FBI Academy and other law enforcement training classes. Through my training and experience, I have developed an understanding of common habits and practices used by those engaged in fraudulent activity.

2. This Affidavit is made in support of a criminal complaint charging BHAVESH PATEL with a violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i) and (ii). Because this Affidavit is made for a limited purpose, I have not set forth each and every fact that I or others have learned over the course of this investigation. Rather, I set forth facts sufficient to establish probable cause that PATEL committed the aforementioned criminal offense.

3. The facts set forth in this Affidavit are based on my own personal knowledge, knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers and other individuals with special training and experience, interviews of witnesses and communication with individuals who have personal knowledge of the events and circumstances described herein, review of documents and records, and my training and experience and that of other experienced investigators. I do not purport to summarize all of the evidence gathered during the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

course of my investigation, nor does the discussion below include all facts known to me or others involved with this investigation.

SUMMARY OF PROBABLE CAUSE

4. The FBI has investigated an intrusion and cyber-attack directed against the protected computer network of a Washington non-profit health services company that operates hospitals and medical center campuses in the South Puget Sound region of Washington State (hereinafter, "Victim Hospital").[1] More specifically, in February 2016, Victim Hospital reported to the FBI that, in August 2013, Victim Hospital's servers were accessed without authorization and manipulated, resulting in a significant system outage at four hospital facilities that lasted about twenty-nine (29) minutes. The compromised servers hosted Victim Hospital's Electronic Medical Records ("EMR") system, which maintains all patient data and records. As set out below, independent forensic analyses by Victim Hospital, third-party consulting firm Navigant Consulting, and the FBI all concluded that BHAVESH PATEL ("PATEL"), a former contractor of Victim Hospital, logged into Victim Hospital's server using another person's credentials and installed a malicious software script onto the server, which caused the EMR system to crash.

5. Between March 2012 and July 2013, PATEL contracted with Victim Hospital as a lead database engineer and administrator.[2] PATEL's responsibilities included the installation and use of electronic medical records (EMR) software developed by Epic Systems for use by Victim Hospital. According to his resume, before contracting with Victim Hospital, PATEL received numerous certifications relating to the installation and use of the Epic Systems EMR software for healthcare providers.

6. At all relevant times, PATEL worked remotely from his residence in South Dakota. Victim Hospital operated a computer network with workstations located in Pierce County, Washington. Accordingly, the conduct described below necessarily caused the transmission of interstate wires and communications.

---

[1] At all times relevant to this matter, and continuing to the present, Victim Hospital has been a wholly-owned subsidiary of a non-profit nationwide network of hospitals.

[2] A staffing agency placed PATEL at Victim Hospital.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

A. VICTIM HOSPITAL'S ELECTRONIC MEDICAL RECORDS SYSTEMS

7. In and around 2013, Victim Hospital stored its EMR data using two record keeping systems in particular: a production (or "PROD") system and a support (or "SUP") system. The PROD system maintained patient medical record information on a real-time basis – *i.e.*, as new patient medical records were created over the course of a day, those records immediately were saved to the PROD system. The medical records information in the SUP system, by contrast, did not update on a real-time basis, but instead was updated at or around the end of each day, through a programming script that caused the information in the PROD system to be copied over into the SUP system on a daily basis. The dual system structure allowed [redacted] to perform routine maintenance to its SUP system during the day without disrupting medical providers' ability to provide services to patients and add new information to the PROD system. As a result, the programming script that caused data in the PROD system to copy over into the SUP system at or around the end of each day served a critical role in Victim Hospital's operations, by ensuring that new medical records information generated over the course of the day was properly stored.

8. A specific line of programming script saved to Victim Hospital's network called for information to be copied from the PROD to the SUP system. That script was programmed to run each day at 2:00 a.m. (MST)[3] using a scheduled task controlled by a network administrator account (referred to as "epicadm"). Victim Hospital's systems logged the script's daily activity and kept track of any errors that occurred while the script was running.

B. PATEL'S ACCESS PRIVILEGES TO VICTIM HOSPITAL'S EMR SYSTEMS

9. In his role as a contractor at Victim Hospital, PATEL had access to the scripts that operated the company's EMR systems, including the PROD and SUP systems. In particular, PATEL was assigned three personalized network login credentials

[3] Unless otherwise stated, all times referred to herein are in Mountain Standard Time (MST).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

or usernames, one of which had elevated access privileges equal to the full administrative privileges on the company's EMR systems.[4] PATEL also was provided with the password for a shared administrator account bearing the name "epicadm" that could be used to perform technical administrative functions across the entire EMR system. PATEL routinely used the "epicadm" account during his time at the Victim Hospital, through which he installed and administered virtually all of the functions that ran on Victim Hospital's EMR systems. PATEL shared these administrative responsibilities with another contractor, M.M., until M.M. left the company in March 2013. M.M. used two personalized login credentials while working at Victim Hospital.

10. Victim Hospital assigned PATEL a laptop to perform his job responsibilities. The laptop enabled PATEL to work remotely from his residence in South Dakota. The laptop assigned to PATEL had the network name "dendmtekl001." By assigning the laptop a network name, Victim Hospital could keep track of its activities on the network, including the dates and times that it logged into the network, the location from which it logged into the network, and the files that it accessed and edited while on the network. Victim Hospital also logged PATEL's remote access to its network by keeping track of his use of a virtual private network (or "VPN") address.

C. PATEL'S JULY 2013 DEPARTURE FROM VICTIM HOSPITAL

11. As explained above, Victim Hospital did not employ PATEL but instead contracted for his services through a staffing firm. PATEL reported to an employee of that staffing firm, P.M., in connection with his project at Victim Hospital.

12. On July 18, 2013, Patel told P.M. over email that he was leaving Victim Hospital. PATEL's email appeared to express displeasure with the Victim Hospital. More specifically, in his email, PATEL "emphasize[d] that my departure was not initiated by me and I really wanted to stay on this adventure and provide my services." PATEL claimed that the management at Victim Hospital "consistently delayed and

---

[4] The company's servers used the Unix operating system, which enables certain users to have "sudo" or "substitute user do" access privileges, through which one user is authorized to exercise certain access privileges assigned to another user.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

postponed" in responding to PATEL's inquiries about whether he could expect a contract extension. PATEL claimed that he resigned from Victim Hospital in order to avail himself of other job opportunities.

13. On July 28, 2013, P.M. told Patel over email that "I will need to retrieve your [Victim Hospital] equipment and badge." The next day, on July 29, Patel responded to Malone's email and claimed that "I got personal emergency and will be back home Aug 9 and will return everything than [*sic*]." Patel did not, however, return his Victim Hospital equipment on August 9, and indeed only returned the equipment on August 16, 2013, after he committed the charged offense using the equipment that he had been asked to return.

D. THE AUGUST 16, 2013 NETWORK INTRUSION AND OUTAGE

14. At about 2:21 a.m. on August 16, 2013, Victim Hospital's medical records system crashed and temporarily became inaccessible to all users. Clinicians working at four Victim Hospital facilities, located in the Western District of Washington, were denied access to the PROD system, which prevented them from accessing patient data on the system and from loading new information onto the system. The system outage continued for approximately twenty-nine (29) minutes, until systems administrators logged into the system and restored its operations. The outage also temporarily prevented hospital administrators from properly admitting six patients into the Emergency Room.

15. As was later discovered, because PATEL had modified the alert email addresses to which system errors ordinarily are reported, Victim Hospital's information technology team did not immediately learn about the outage through an email alert. Instead, according to a Victim Hospital representative, a clinician called the company's IT department to report the outage.

16. At approximately 2:50 a.m., approximately twenty-nine (29) minutes after the system outage began, a Victim Hospital database administrator was able to restore the EMR system to its normal operations and preserved data and log files.

17. After the intrusion, Victim Hospital's Incident Response and Forensic unit conducted a forensic examination to determine the cause of the system outage. Victim

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Hospital's forensic examination included a review of system log files that track the identities of users who access the company's servers, the dates and times of such access, and the users' activity upon accessing the servers. I have reviewed a written report prepared by Victim Hospital, which summarizes the methods used by the company's forensic examiners, the digital evidence they uncovered, and their findings. An FBI computer scientist has also reviewed the report's findings and the original data maintained by Victim Hospital, confirming that those findings accurately describe the digital evidence extracted from Victim Hospital's network.

18. More specifically, Victim Hospital's forensic examiners reviewed the critical "log files" on the company's network, which record virtually every event that occurs on the network. For instance, the network log files keep track of the dates and times when users log into the network, the usernames they use when logging in, the network names assigned to the computers from which they access the network, the external IP addresses from which they log in, the internal IP addresses that the network assigns to their computers, and the files that they access and manipulate upon logging in.

E. EVIDENCE OF PATEL's ROLE IN THE NETWORK INTRUSION AND OUTAGE

19. Through its review, Victim Hospital uncovered evidence that PATEL accessed Victim Hospital's servers on August 16, 2013 and caused the system outage by attempting to manipulate the process by which data copied from the PROD to the SUP systems.

20. Below is a timeline of certain pertinent events:

a. On July 17, 2013, PATEL logged into Victim Hospital's network using his own username, elevated his access to an administrative account, and modified the access privileges and password for one of the two usernames assigned to M.M (hereinafter the "M.M. account").[5] In particular, PATEL assigned the M.M. account

[5] The evidence that PATEL logged into Victim Hospital's servers on July 17 includes the following: (a) the login IP used by PATEL was the same IP address assigned to PATEL's VPN access; and (b) the username that accessed the Victim Hospital network was "bpatel," which had been assigned to PATEL.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

access to the scripts associated with the daily transfer of data from the PROD to SUP systems. PATEL also authorized the M.M. account to log into the company's systems remotely – i.e., from computers that were not physically connected to the company's servers. PATEL then logged into the M.M. account remotely from his own laptop computer, in an apparent attempt to make sure that the changes he made to the account had taken effect.

b. On July 18, 2013, PATEL emailed P.M. to inform him about his departure from Victim Hospital.

c. On July 28, 2013, P.M. emailed PATEL about the return of PATEL's Victim Hospital equipment and credentials.

d. At approximately 12:32 a.m. on August 16, 2013, PATEL initiated a remote VPN connection to Victim Hospital's network using his own login username ("bpatel"). Victim Hospital's network tracked the public Internet Protocol ("IP") address from which PATEL logged into the network as 208.107.42.101, which was an IP address assigned by Midcontinent Communications, an internet service provider in South Dakota, to PATEL. The network also tracked the laptop that PATEL used to log into the network as dendmtekl001, which (as explained above) was the laptop that had been assigned to PATEL and which PATEL had failed to return to Victim Hospital in a timely manner. Upon logging into Victim Hospital's network, PATEL's computer was assigned an internal IP address that allowed the computer to communicate with internal network resources.

e. One minute after initiating his VPN session under his own username and after being assigned an internal IP address by the company's network, PATEL logged into the company's network using M.M. account and the password for the M.M. account that PATEL had reset on July 17, 2013. Victim Hospital's network recorded the login under the M.M. account as having occurred during the same remote-access session that PATEL initiated under his own username (and from the same internal IP address that had been assigned to PATEL's computer). After logging in as M.M., PATEL ran a command to elevate the M.M. account's access privileges, and then logged in under the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

"epicadm" administrator username. PATEL then copied certain data from the SUP to the PROD system, in an apparent attempt to test whether files could be copied from the backup system to the primary system. PATEL logged out of the network at approximately 12:42 a.m.

f. Approximately thirty minutes later, at 1:19 a.m., PATEL again logged into the Victim Hospital network using the "epicadm" administrator username. Victim Hospital's network traced this login to the same virtual private network IP address that PATEL had used when logging into the network between 12:32 a.m. and 12:42 a.m. While logged in under the administrator account, PATEL accessed a file that contained two legitimate email addresses to which all network errors would be reported, changed those email addresses to nonexistent email addresses, and then manipulated the file's metadata to make it appear as if he never had edited it. In my experience and training, PATEL's effort to change the email addresses to which network errors would be reported and to eliminate any record that he did so demonstrates his intent to prevent Victim Hospital's network administrators from timely responding to, remedying, and investigating network failures. At approximately 1:23 a.m., PATEL logged out of the administrator account.

g. Approximately fifteen minutes later, at 1:38 a.m., PATEL initiated a new VPN session. Victim Hospital's network logged the fact that PATEL initiated this session using his own username ("bpatel") from an IP address in South Dakota.[6] Upon initiating the VPN session, Victim Hospital's network assigned PATEL's computer an internal IP address from which it could communicate with internal network resources. At 1:44 a.m., PATEL logged into the "epicadm" administrator account from the internal IP address that had been assigned to his computer six minutes earlier. While logged in as an administrator, PATEL looked up information about access permissions to the file directory in Victim Hospital's network that contained the script pursuant to which data

[6] As explained above, records produced by Midcontinent Communications, an internet service provider in South Dakota, show that PATEL was the subscriber associated with the IP address during August 2013.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

copied from the PROD to SUP system. PATEL also briefly examined a log file regarding the script's operation.

h. At approximately 2:05 a.m., while logged in under the "epicadm" administrator username and from the same internal IP address that Victim Hospital's network had assigned his computer, PATEL modified the access rights to the file on Victim Hospital's network that contained the script pursuant to which data was copied from the PROD system to the SUP system. PATEL provided "wide open access" to the file, such that any user could edit the file. PATEL then logged into the Victim Hospital network using the M.M. account.[7]

i. After logging in as M.M., PATEL initiated a separate session under the "epicadm" administrator account, such that he was effectively logged in as M.M. with administrator privileges. While operating as an administrator, PATEL accessed the file containing the scripts that were responsible for copying data from the PROD to the SUP systems.[8] The network log file shows that the content of the script that ran at 2:20 a.m. differed in two significant ways from the script that regularly had run on previous days: (i) ***first***, rather than attempting to copy data from the PROD to the SUP system, the revised script attempted to copy data from the SUP to the PROD system – i.e., in essence reversing the direction of the data back-up protocol; and (ii) ***second***, rather than being scheduled to run at 2:00 a.m., the revised script was scheduled to (and did) run at 2:20 a.m. In effect, PATEL modified the script to overwrite all of the new medical data from the previous day with older data contained on the SUP system.

j. At 2:20 a.m. (and twenty minutes after its normal runtime), as PATEL directed, the script (as revised by PATEL) attempted to run, but then aborted,

---

[7] Victim Hospital recorded the mmubeen1 login as having occurred from the same internal IP address that PATEL's computer had been assigned minutes earlier. Network logs also show that the M.M. account logged in from the dendmtekl001 computer – i.e., the network name assigned to PATEL's laptop.

[8] Victim Hospital's network kept logs of the fact that a computer using the internal IP address that PATEL had been assigned at the start of his VPN session did all of the following, while logged in as an administrator: (a) started a secure file transfer protocol session at 2:17 a.m.; (b) loaded the file containing scripts into a program that would have permitted PATEL to edit the file at 2:17 a.m.; and (c) again loaded the file containing scripts into a program that would have permitted PATEL to edit the file at 2:26 a.m.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

causing a system-wide outage. As noted above, Victim Hospital's EMR systems crashed and became inaccessible as a result of PATEL's conduct. More specifically, four Victim Hospital facilities located in this District lost access to the patient data and records. Moreover, because of PATEL's unauthorized modifications, Victim Hospital system administrators did not receive an automated alert notification email regarding the system outage.

k. At 2:26 a.m., PATEL, logged in under M.M. account (with administrator privileges), again edited the script and restored it to its previous state, such that the script again called for data to be backed up from the PROD to the SUP system at 2:00 a.m. each day. In addition to restoring the script, PATEL took other apparent efforts to cover his tracks. In particular, PATEL manipulated the metadata on a log file that kept track of the dates and times of any changes to the scripts that he edited.

21. After preparing its final forensic report, Victim Hospital retained the services of a third-party forensic examiner named Navigant Consulting. Navigant examined the network log files and other records and reached the same conclusions that Victim Hospital's forensic team reached regarding PATEL's access to the network, his manipulation of scripts to interfere with Victim Hospital's normal process for backing up medical records information, and his attempts to cover up evidence of his activity.

F. PATEL'S CONDUCT AND STATEMENTS AFTER THE INTRUSION

22. After the network intrusion and outage on August 16, 2013, PATEL engaged in conduct and made statements, all of which serve as additional evidence that he committed the crime set out above. More specifically:

1. Immediately after the Intrusion, PATEL Wiped His Laptop and Returned It to Victim Hospital

23. After delaying returning his company laptop and credentials, as requested, PATEL abruptly wiped his device and mailed it to Victim Hospital shortly after the network intrusion. More specifically, several hours after committing the intrusion on

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

August 16, 2013, PATEL sent a text message from his personal cellular phone to P.M.[9] In that message, PATEL claimed that he had sent the laptop and other items to Victim Hospital's offices in Colorado, via FedEx.[10]

24. Before returning the laptop to P.M., PATEL deleted all of the data on the laptop, including all of the digital records of his activity on the laptop. According to the company's forensic report, Victim Hospital determined that PATEL erased all of the data on his company laptop because the laptop contained no file content whatsoever upon receipt.

25. According to Victim Hospital, on about September 7, 2013, PATEL admitted that he ran a program that erased all of the content on his hard drive before mailing the laptop to P.M. In addition, when I interviewed PATEL at his residence in April 2017, discussed below, PATEL admitted that he wiped his hard drive and claimed that he did so because his laptop contained patient medical reports containing personally identifiable information.

2. PATEL Initially Admitted He Accessed Victim Hospital's Servers and Sought Help Potentially to Conceal Evidence of That Access

26. On September 3, 2013, after reviewing logs and digital records of PATEL's conduct, Victim Hospital's network security director, G.B., called PATEL to interview him. During that call, PATEL acknowledged accessing Victim Hospital's servers after his departure, but claimed that he only did so in order to organize (and clean up) his emails and provide some remaining documentation to the company. PATEL did not, however, admit that he accessed the servers on August 15 or August 16, 2013. PATEL promised to consult his notes and speak again with G.B. about G.B.'s concerns at a later date.

---

[9] The text message was signed "Bob Patel." It also was sent from a telephone number that PATEL provided (as his own) in his July 18, 2013 email to P.M.

[10] PATEL's text to P.M. included the FedEx tracking number for the package containing the equipment. FedEx tracking records show that the package shipped from Sioux Falls, South Dakota on August 16, 2013 and arrived in Colorado on August 20, 2013.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

27. On September 3, 2013 (the same day as his first call with G.B.), PATEL called a former Victim Hospital colleague and asked that individual for guidance about how to edit the servers' log files. The former colleague reported the call both to a senior IT administrator at Victim Hospital (and later to me during an interview in April 2017). The former colleague recounted that PATEL requested that he ask another person in the IT department about how to manipulate log-file information, and that PATEL followed up with a text message and another (unanswered) call a few days later.

28. On about September 6, 2013, PATEL and the former colleague connected again by phone. According to the former colleague, during that call, PATEL, among other things, was curious to know if anyone was monitoring Victim Hospital's servers. In my experience and training, PATEL's inquiries about modifying log files at or around the time that Victim Hospital confronted him about his involvement in the August 16, 2013 intrusion is evidence of his interest in potentially deleting or altering evidence of his wrongdoing.

29. On about September 7, 2013, PATEL again spoke with Victim Hospital network security director, G.B. According to G.B., G.B. confronted PATEL with the digital evidence that PATEL had committed the network intrusion on August 16, 2013. In response, PATEL repeatedly told G.B. that "if I had accessed the system, it would not have been with the intent of damaging the system." PATEL later admitted that he accessed Victim Hospital's network on August 16, 2013, but claimed that he did so only in order to organize his emails, complete a few remaining tasks, and copy scripts from the company's servers to his own laptop. PATEL also denied editing the scripts that directed the transfer of data from the PROD system to the SUP system and, indeed, claimed that he did not interfere with the ordinary operation of those daily processes.

30. PATEL's story seemed to evolve as G.B. provided additional information. Ultimately, near the end of the September 7, 2013 call with G.B., PATEL then told G.B. that if Victim Hospital assured PATEL that it would not pursue the matter further, then PATEL would disclose to G.B. all of the information that PATEL had about the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

intrusion. PATEL also expressed concerns about the legal implications of making further statements to G.B. about the intrusion.

3. PATEL's April 11, 2017 Interview with the FBI

31. On April 11, 2017, I interviewed PATEL at his residence in South Dakota. PATEL agreed to voluntarily speak with me. PATEL admitted that he ceased doing official work for Victim Hospital by the end of July 2013, but asserted that he held on to his laptop in order to make copies of scripts that he had created while working for Victim Hospital. PATEL claimed that he logged into Victim Hospital's servers in August 2013 with the intent to use a file-transfer protocol ("FTP") to copy information from Victim Hospital's servers to his own laptop. PATEL asserted, however, that he mistakenly copied scripts from his laptop to the company's servers. PATEL attributed this purported mistake to fatigue, as a result of having worked long hours before logging onto the network. Despite claiming that it was a purported mistake, PATEL confirmed that no other individual could have been responsible for the network outage that occurred on August 16, 2013.

32. During his interview, PATEL claimed that he could not recall numerous events that were recorded by the company's servers (and that are discussed above). For instance, PATEL claimed not to remember modifying the email address to which any errors would have been reported. PATEL also claimed not to remember modifying the password and access credentials for the M.M. account on July 17, 2013. In addition, PATEL claimed not to remember calling and sending text messages to a former colleague with regard to his request to modify the servers' log files.

33. As set out above, in my experience and training, PATEL's assertion that he only intended to copy files from the Victim Hospital's network to his own laptop simply cannot be reconciled with his actual conduct on August 16, 2013. Specifically, none of PATEL's activity on the Victim Hospital network is consistent with an effort to retrieve data from the network. Rather, PATEL modified scripts on the network that controlled the direction in which EMR records would be copied at the end of each day.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

Based on the above facts, I respectfully submit that there is probable cause to believe that BHAVESH PATEL did knowingly and intentionally commit the criminal offense of Intentional Damage to a Protected Computer, in violation of Title 18, United States Code, Sections 1030(a)(5)(A) and (c)(4)(B)(i)(I), (II), (IV) and (VI) and (ii).

Michael D. Brown, Complainant
Special Agent, FBI

Based on the Complaint and Affidavit sworn to before me, and subscribed in my presence, the Court hereby finds that there is probable cause to believe the Defendant committed the offense set forth in the Complaint.

Dated this 9th day of May, 2018.

David W. Christel
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970